EJK:SK
F.#2013R01878

14 MISC 090

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- - - - - - - - - - - - - - - - - - X

IN THE MATTER OF THE SEARCH OF:

THE PREMISES KNOWN AND DESCRIBED AS AN LG CELLULAR TELEPHONE, MODEL P769, IMEI 013647004306885

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

(T. 21, U.S.C., §§ 841(a)(1) and 952(a))

- - - - - - - - - - - - - - - - - - X

EASTERN DISTRICT OF NEW YORK, SS:

CHRISTOPHER McKELVY, being duly sworn, deposes and states that he is a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is located in THE PREMISES KNOWN AND DESCRIBED AS AN LG CELLULAR TELEPHONE, MODEL P769, IMEI 013647004306885 (the "DEVICE"), further described in Attachment A, the things described in Attachment B, which constitute evidence, fruits, and instrumentalities of importing a controlled substance into the United States from a place outside thereof, in violation of Title 21, United States Code, Section 952(a), and possessing with intent to distribute a controlled substance, in violation of Title 21, United States Code, Section 841(a)(1).

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI") and have been a Special Agent with HSI for approximately 5 years. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for federal narcotics offenses and narcotics trafficking into the United States. These investigations are conducted both in an undercover and overt capacity. I have participated in investigations involving search warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from my own observations, reports made to me by other law enforcement officers, and review of records from HSI and other government agencies. In addition, when I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated.

3. HSI is investigating the unlawful possession with intent to distribute narcotics and importation of narcotics.

[1] Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

BACKGROUND

4. On or about November 6, 2013, Christina Cordova (the "Courier") arrived at John F. Kennedy International Airport ("JFK") aboard Caribbean Airlines Flight No. 520 from Port of Spain, Trinidad.

5. After the Courier's arrival, United States Customs and Border Protection ("CBP") officers selected the Courier for an enforcement examination. The Courier presented a green suitcase and two yellow carry-on bags for inspection (collectively, the "Luggage"). The Courier informed CBP officers, in sum and substance and relevant part, that the Luggage and everything within it belonged to the Courier, that the Courier had purchased all of the items in the Luggage, and that the Courier had packed the Luggage herself.

6. In the Luggage, CBP officers found eight boxes marked as containing Tortuga Caribbean Rum Cakes (the "Boxes"). CBP officers probed the cake inside one of the Boxes and discovered a white powdery substance. The white powdery substance field-tested positive for cocaine. CBP officers also discovered a white powdery substance concealed in each of the other Boxes. Law enforcement officers recovered a total gross weight of approximately 3,675.6 grams of cocaine from the Boxes.

7. The Courier was arrested. The Courier was read her Miranda rights and invoked her right to counsel. Subsequently, the Courier expressed that she wanted to speak to law enforcement officers. The Courier was re-read her Miranda rights; she waived those rights and agreed to speak with law enforcement officers without an attorney present. In post-arrest statements, the Courier stated, in sum and substance and relevant part, that: the Courier wanted to go on vacation and consulted a co-worker in Elizabeth, New Jersey (the "Recruiter") about possible destinations; the Recruiter suggested that the Courier go to

Trinidad and informed the Courier that she (the Recruiter) had a friend in Trinidad (the "Supplier") who could facilitate the Courier's trip; the Courier paid for the trip and her hotel using her credit card; and upon arrival, the Courier met with the Supplier, who picked the Courier up from the airport, took her to the hotel, and took her around shopping and elsewhere. The Courier further stated, in sum and substance and relevant part, that: the Courier bought the Boxes at a store; the Courier packed the Boxes in the Luggage; and the Supplier gave the Courier the number of an individual in New York (the "Pick-Up Guy") who could pick the Courier up once she returned to New York and if she needed a ride home.

8. Subsequently, the Courier stated that she wished to speak with law enforcement officers again. The Courier stated, in sum and substance and relevant part, that: the Recruiter told the Courier that the Courier could earn $3000 for bringing gold into the United States from Trinidad; the Recruiter told the Courier that she (the Recruiter) had taken trips for the Supplier before; the Courier paid for her airplane ticket to Trinidad on Thursday (October 31, 2013, two days prior to departure) with money that the Supplier had sent her via Western Union; the Supplier paid for the Courier's hotel in Trinidad; the Supplier gave the Courier the Boxes on the night before she left Trinidad (the Courier did not buy them); the Supplier told the Courier that the Boxes contained Guyana gold that the Supplier wanted to smuggle into the United States; the Courier asked the Supplier if the Boxes contained drugs and the Supplier responded that they did not contain drugs, just gold; and the Supplier instructed the Courier to call the Pick-Up Guy upon arrival in New York and informed the Courier that the Pick-Up Guy would pick up the Courier and take the Boxes from her.

9. At the time of the enforcement examination, the Courier had the DEVICE in her possession. A search of the DEVICE revealed:

a. the telephone numbers of the Recruiter, the Supplier, and the Pick-Up Guy among the list of phone contacts;

b. a photograph of a business card for a hotel in Trinidad containing the hotel's telephone numbers and email address;

c. two outgoing telephone calls made on the morning of November 6, 2013, shortly after the Courier's arrival at JFK;

d. a WhatsApp text message conversation dated October 31, 2013, referencing Western Union payment information;

e. a photograph taken on November 1, 2013, of a WhatsApp text message from the Courier to the Supplier stating "Ok cool";

f. photographs taken on November 4, 2013, of flight itineraries and airfares for various flights from Port of Spain, Trinidad to JFK departing on November 6-7, 2013;

g. an unsent outgoing text message to the Pick-Up Guy dated November 6, 2013, stating "Just got off the plane."

10. On December 2, 2013, a grand jury in the Eastern District of New York returned an indictment charging the Courier with one count of importation of cocaine (in violation of 21 U.S.C. § 952(a)) and one count of possession of cocaine with intent to distribute (in violation of 21 U.S.C. § 841(a)(1)).

11. Based on my training and experience and discussions with other law enforcement officers, I know that individuals involved in the importation and possession with intent to distribute narcotics often do not act alone and often communicate with coconspirators by means of cellular telephones such as the DEVICE. They commonly maintain records that

reflect names, addresses, or telephone numbers of their associates in their cellular telephones. They also commonly maintain records of communications such as call logs, chats, text messages and WhatsApp messages in their cellular telephones. They also commonly take photographs of themselves, their associates, or their property using their cellular telephones. These individuals usually maintain these records of communication and photographs in their possession and in their cellular telephones.

12. Based on my knowledge, training, and experience, I know that the DEVICE can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the DEVICE. This information can sometimes be recovered with forensic tools.

13. Upon the Courier's arrest, law enforcement officers seized the DEVICE. Since its seizure, the DEVICE has been in law enforcement custody. There is therefore probable cause to believe that the DEVICE contains evidence, fruits, and instrumentalities of federal crimes.

TECHNICAL TERMS

14. Wireless telephone (or mobile or cellular telephone): A handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land-line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving and storing text messages and

email; taking, sending, receiving and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device, and a wide variety of applications, also known as "apps," which may store the user's preferences and other data. Such apps may include Facebook, Twitter, WhatsApp and other social media services. WhatsApp is a cross-platform mobile messaging application which allows users to exchange written messages between smartphones over a network, and included messages can contain image, video and sound content.

15. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or other electronic device, such as the DEVICE, that connects to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static-that is, long-term- IP addresses, while other computers have dynamic - that is, frequently changed - IP addresses.

16. Based on my research, I know that the DEVICE provides not only phone and text message services, but can also be used to send and receive emails; access the Internet; track GPS data; take, store and share photographs and videos; and use a wide variety of apps, such as Facebook, Twitter, WhatsApp and many others. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the DEVICE.

TECHNICAL BACKGROUND

17. As further described in Attachment B, this application seeks permission to locate not only data that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence can be recovered from the DEVICE because:

a. Data on an electronic device can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the device that show what tasks and processes were recently active. Web browsers, email programs, and instant messaging/"chat" programs store configuration information on the device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the device was in use. Electronic devices can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on an electronic device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, instant messaging or chat logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the electronic device at a relevant time.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant. This process of conducting a forensic examination of an electronic device requires examination of all of the data on the device.

e. Further, in finding user attribution evidence, sometimes it is necessary to establish that a particular thing is not present on an electronic device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses an electronic device to illegally import narcotics, the individual's electronic device may generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the device was used; data that was sent or received; notes as to how the criminal conduct was achieved;

records of Internet discussions about the crime; and other records that indicate the nature of the offense.

18. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

19. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve intrusion into a physical location. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

20. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that on the DEVICE there exists evidence of crimes. Accordingly, a search warrant is requested.

21. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application including the application and search warrants. I believe that sealing these documents is necessary because the disclosure of the existence of this warrant would provide confederates of the Courier an opportunity to flee from prosecution, change patterns of behavior such as by changing their cell phone numbers, and otherwise seriously jeopardize the ongoing investigation. Based upon my training and experience, I have learned that criminals actively search for criminal

affidavits and search warrants via the internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly through online forums. I have also learned that criminals often change phone numbers as a means of evading detection by law enforcement. Therefore, premature disclosure of the contents of this affidavit and related documents will seriously jeopardize the investigation, including by giving individuals the opportunity to continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates.

AUTHORIZATION REQUEST

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS AN LG CELLULAR TELEPHONE, MODEL P769, IMEI 013647004306885.

IT IS FURTHER REQUESTED that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application including the application and search warrants.

Dated: Brooklyn, New York
January 24, 2014

Christopher McKelvy
Special Agent, HSI

Sworn to before me this
24th day of January, 2014

s/Marilyn D. Go

THE HONORABLE MARILYN D. GO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property To Be Searched

The property to be searched is an LG CELLULAR TELEPHONE, MODEL P769, IMEI 013647004306885, hereinafter the "DEVICE." This warrant authorizes the forensic examination of the DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things To Be Seized

All information obtained from DEVICE will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes fruits, evidence and instrumentalities of importing a controlled substance into the United States from a place outside thereof, in violation of Title 21, United States Code, Section 952(a), and possessing with intent to distribute a controlled substance, in violation of Title 21, United States Code, Section 841(a)(1), including for the time period from October 1, 2013 to present:

1. All records and information on the DEVICE described in Attachment A, including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, WhatsApp messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of importing a controlled substance into the United States from a place outside thereof, in violation of Title 21, United States Code, Section 952(a), and possessing with intent to distribute a controlled substance, in violation of Title 21, United States Code, Section 841(a)(1);

2. Evidence of user attribution showing who used or owned the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software;

5. Evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence;

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;

7. Evidence of the times the DEVICE was used;

8. Passwords, encryption keys, and other access devices that may be necessary to access the DEVICE; and

9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of importing a controlled substance into the United States from a place outside thereof, in violation of Title 21, United States Code, Section 952(a), and possessing with intent to distribute a controlled substance, in violation of Title 21, United States Code, Section 841(a)(1).

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.